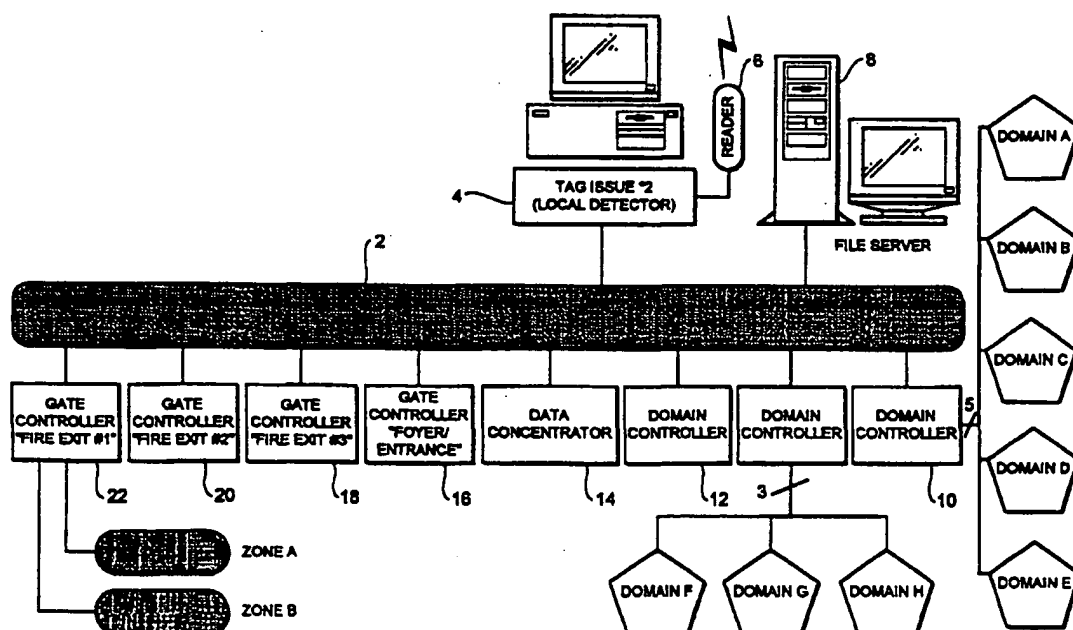




## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<b>(51) International Patent Classification <sup>6</sup> :</b> <b>G07C 9/00, G01V 15/00</b>	<b>A1</b>	<b>(11) International Publication Number:</b> <b>WO 97/01154</b> <b>(43) International Publication Date:</b> 9 January 1997 (09.01.97)
<b>(21) International Application Number:</b> PCT/GB96/01516 <b>(22) International Filing Date:</b> 21 June 1996 (21.06.96)  <b>(30) Priority Data:</b> 9512562.1                      21 June 1995 (21.06.95)                      GB 9512563.9                      21 June 1995 (21.06.95)                      GB  <b>(71) Applicant (for all designated States except US):</b> MEDESTATE LTD. [BS/BS]; Cumberland House, 27 Cumberland Street, P.O. Box N8308, Nassau (BS).  <b>(72) Inventors; and</b> <b>(75) Inventors/Applicants (for US only):</b> MITCHESON, Mark [GB/GB]; Cemetery Park Lodge House, Loftus, Cleveland TS13 4LZ (GB). KEVAN, Robert, Andrew [GB/GB]; 51 Emmaville, Ryton, Tyne & Wear NE40 3TR (GB). GREN-SIDE, Mark, Nicholas [GB/GB]; 59a Cadogan Gardens, London SW3 2RA (GB).  <b>(74) Agents:</b> DRIVER, Virginia, Rozanne et al.; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).		<b>(81) Designated States:</b> GB, JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  <b>Published</b> <i>With international search report.</i>

(54) Title: A TAG AND TAG MONITORING SYSTEM



(57) Abstract

A tag monitoring system and a tag for use therein is disclosed. A system is provided in which the location of tag holders can be detected in different regions within a building or other site. This is achieved by using a plurality of beacon sets each defining a domain within a monitored volume. The beacon sets can be sequentially selected to poll their domain to uniquely identify any tags within the domain and to update location data defining the location of wearers of the tags accordingly.

Title of the InventionA TAG AND TAG MONITORING SYSTEMField of the Invention

The present invention relates to a tag monitoring system and to a tag for use therein.

Background of the Invention

One aim of the invention is to provide a system in which the location of tag holders can be detected in different regions within a building or other site.

Summary of the Invention

According to the present invention there is provided a tag monitoring system comprising: a tag issue unit for issuing a plurality of tags, each tag being uniquely identifiable; a system controller for holding the identity of each issued tag with data identifying the location of that tag within a monitored volume; a plurality of beacon sets defining a domain within the monitored volume, the beacons within each set each having a transmit antenna and a receive antenna for transmitting and receiving respectively electromagnetic signals in the domain, wherein beacons within one set are arranged at different locations from beacons in the other sets to substantially avoid dead zones within the domain, and wherein the system controller comprises switching means for sequentially selecting said beacon sets to poll the domain to uniquely identify any tags within the domain and to update said location data accordingly.

Thus, each person to be monitored is issued with a tag which is subsequently identified when the tag wearer enters a domain. Once the presence of a tag in the domain is

- 2 -

identified, a detection record can be created detailing the location of the wearer and the date and time at which detection was made.

Arrangement of beacon sets to avoid dead zones ensure there is full coverage in each domain. Thus, the domains do not need to be physically defined and could even cross other physical boundaries.

In most implementations there are a plurality of domains, each domain being defined by such a plurality of beacon sets. In that event, the system controller is operable to poll all of the domain to determine the location of tags and to keep a detection record.

The monitored volume can be defined by a physical boundary having at least one exit zone, there being arranged at said exit zone an internal beacon set and an external beacon set on opposed sides of the exit zone in relation to the physical boundary to define a gate region. In that event, the system controller is operable to poll said gate region to detect when any tags leave the monitored volume.

The system controller can be arranged to generate a warning signal when a tag leaves the monitored volume.

The system controller can comprise a domain controller for polling the or each domain and a separate data concentrater for holding up-to-date information concerning the identity of each tag and its location.

The data concentrater and the domain controller can be separately connected to a network which allows communication between them. The tag issue unit may also be connected to that network.

- 3 -

The monitored volume can include a plurality of domains, with a plurality of domain controllers, each domain controller monitoring a plurality of said domains.

Each tag issued by the tag issue unit can have stored therein a unique code identifying the tag. In that case, the system controller is operable to poll the or each domain by issuing a sequence of codes for transmission by the transmit antennas of the beacon sets and for awaiting any responses via the receive antennas of the beacon sets, a response being issued by a tag whose stored code matches the transmitted code.

The system controller can hold with the identification of each tag an expiry time for that tag, the expiry time representing the time at which a holder of the tag can no longer validly remain in the monitored volume and is operable to generate an expiry signal to that tag when the expiry time is reached.

Tags using electromagnetic signals can be used to monitor the locations and movements of people on a site or in a building.

The present invention provides in another aspect a tag for use in a tag monitoring system comprising: a receiver for receiving an electromagnetic signal from a system controller; a transmitter for transmitting electromagnetic signals as response to received signals; logic circuitry for controlling the responses of the tag; and a visual indicator controlled by the logic circuitry so that it can be activated in response to electromagnetic signals transmitted from the system controller.

The visual indicator can be a light-emitting diode or other light which is turned on continuously or to flash when activated.

- 4 -

Each tag can include a store holding a code uniquely identifying the tag and a comparator for comparing incoming codes from the system controller with the stored code, wherein a response is issued if the incoming code matches the stored code.

The present invention also provides a tag monitoring system for monitoring the locations of tags within a volume, wherein the system controller holds the identification of each tag within the monitored volume together with expiry data denoting an expiry time beyond which the holder of the tag should no longer validly remain in the monitored volume, the system controller being operable to issue an expiry signal to a tag when its expiry time is reached, said expiry signal causing the visual indicator to be activated.

Where the tag includes a store holding a unique code, the expiry signal is issued with the code uniquely identifying the tag for which the expiry time has been reached.

The system controller includes a clock so that the real time can be compared with the expiry times of tags to issue the expiry signal when the expiry time for an identified tag has been reached.

Alternatively or additionally to using the visual indicator to indicate expired times, the system controller can transmit a signal to actuate the visual indicators on all tags in an emergency situation.

For a better understanding of the present invention and to show how the same may be carried into effect reference will now be made by way of example to the accompanying drawings.

- 5 -

Brief Description of the Drawings

Figure 1 is a block diagram of a tag monitoring system;

Figure 1a is a diagram of a gate zone;

Figure 2 illustrates how a domain is defined using beacon sets;

Figure 3 is a diagram representing how the beacon sets are activated in each domain;

Figure 4 is a block diagram of elements of a domain controller;

Figure 5 is a diagrammatic sketch indicating operation of the domain controller; and

Figure 6 is a block diagram of the main components of a tag for use in the system.

Description of the Preferred Embodiment

Figure 1 is a block diagram of a tag monitoring system. Reference numeral 2 denotes a communication network by means of which the components of the monitoring system are able to communicate. The monitoring system comprises a tag issue unit 4 connected to a tag reader 6. The tag issue unit 4 is connected to the network 2. Also forming part of the monitoring system are first and second domain controllers 10,12 which are each connected to the network 2. There is also a data concentrator 14 connected to the network 2 and four gate controllers 16,18,20,22 each connected to the network 2. It will be appreciated from the following description that the number of domain controllers and gate controllers can be selected according to the requirements of the monitoring system. Each gate controller defines two zones indicated in Figure 1 as zone A and zone B. Those zones are separated by a physical boundary. These are illustrated only for the gate controller 22 but will be defined for each of the gate controllers 16,18 and 20. The first domain controller 10

- 6 -

is in communication with five domains labelled Domain A to Domain E respectively. The second domain controller 12 is connected to three domains labelled Domain F to Domain H. These domains are not defined by physical boundaries but by a scanning system described in more detail hereinafter.

Tags are issued at the tag issue unit 4. Each tag includes a receiver and transmitter for respectively receiving and transmitting radio frequency (RF) signals allowing the tag to communicate with the monitoring system.

An overall volume to be monitored is defined by a physical boundary. That boundary has a set of exits/entrances, each of which is monitored by a gate controller. Each gate controller has two separate sets of antennas, one monitoring zone A, for example inside the volume, and the other monitoring zone B, outside the volume.

Figure 1a is a diagram in the region of such an exit/entrance. Reference numeral 1 denotes the wall constituting the physical boundary defining the exit/entrance 3.

Each of the domains A to H is a sub-volume within which the main volume in which tags may be detected. The domains are within the physical boundary. The domains are defined by tag detection antennae (beacons) distributed throughout the volume. The beacons are arranged in a plurality of beacon sets, with each set comprising a plurality of beacons connected to be activated together. Depending on the size and nature of the domain to be defined, any number of beacon sets can be utilised. The beacon sets are arranged so that there is full coverage throughout the domain volume. Figure 2 shows a domain having two beacon sets. The first beacon set BEACON SET 1 is shown shaded on the left hand side of Figure 2 and

- 7 -

comprises five beacons whose area of coverage is illustrated diagrammatically by the outer circumferences of the circles. Reference numeral 24 denotes a beacon. The diagram on the right hand side of Figure 2 represents the second beacon set BEACON SET 2 having four beacons arranged at different locations to give a different radar coverage to that given by BEACON SET 1.

The monitoring system is arranged so that it is possible to detect the location of tags within the volume covered by the monitoring system. To this end, each gate zone and domain is polled to determine whether or not tags are in the zone or domain respectively.

For the purposes of polling each domain, each domain controller has transmit and receive beacon set controlling switches 26,28 illustrated diagrammatically in Figure 3. There is a set of such switches for each domain to be polled by the domain controller. The transmit switch 26 has four terminals T1 to T4 and the receive switch has four terminals R1 to R4. Each beacon 24 consists of a transmit antenna  $A_t$  and a receive antenna  $A_r$ . The transmit antennas  $A_t$  of BEACON SET 1 are connected to the first terminal T1 of the transmit switch 26. The receive antennas  $A_r$  of the BEACON SET 1 are connected to terminal R1 of the receive switch 28. Similarly, the transmit antennas of BEACON SET 2 are connected to the second terminal T2 of the transmit switch 26, and transmit antennas of subsequent beacon sets are connected to the remaining terminals T3,T4. Likewise, the receive antennas of BEACON SET 2 are connected to the second terminal R2 of the receive switch 28. The receive antennas of subsequent beacon sets are connected to the remaining receive terminals R3,R4. In operation, transmit switch 26 is firstly connected to the first terminal T1 and the receive switch 28 is connected to its first terminal R1. A signal is transmitted through the



- 8 -

transmit antennas  $A_t$  of the first beacon set 1 and any signals received are supplied to the receive switch 28 from the receive antennas. The transmit signal is denoted  $T_x$  and the received signal is denoted  $R_x$ . Then, the transmit and receive switches 26,28 are connected to the second terminals T2,R2 and the process of transmitting a signal  $T_x$  and waiting for any receive signal  $R_x$  is repeated. Once all beacon sets within a domain have been activated, the transmit and receive switches return to the first terminal to begin the sequence again.

As explained above, each domain controller has a plurality of sets of transmit and receive switches 26,28, there being one set for each domain to be polled by the domain controller. Figure 4 is a block diagram of the main components of each domain controller. The sets of transmit and receive switches are contained within a router 30. The router 30 has a plurality of ports (five in the case of domain controller 10 and three in the case of domain controller 12). These ports are denoted in Figure 4 as P1 to P5. Each port is bidirectional and is capable of receiving and transmitting signals between the domains and the domain controller. The router 30 is connected via a two-way communication path to an interface 32. The interface itself communicates with a microprocessor 34. The microprocessor 34 is also connected to the network 2 via a two-way communication path 36. The microprocessor 34 controls polling of the domains by the domain controller.

Figure 5 is a diagram for the purposes of explaining how the microprocessor 34 operates to control polling of domains. It will be appreciated that Figure 5 is diagrammatic only and that the processes and databases illustrated in Figure 5 may be organised in any appropriate manner within the microprocessor 34. There are a set of poll databases 40 each

- 9 -

holding up-to-date information concerning the locations of tags issued by the tag issue unit 4. There is a poll database for each domain controlled by the domain controller. Each poll database 40 holds information concerning tag IDs, the location of the tags, the time and date. When a tag is first issued by the tag issue unit, its identity is read by the tag reader 6, the system is set to mark the tag as active and its location is set to a default location, e.g. INSIDE. A tag detection process updates the poll databases as each domain is polled. The tag detection process 42 causes the microprocessor to output signals to the router 30 to control connection of the transmit and receive switches 26,28 and generates the signals  $T_x$  to be transmitted. These signals are referred to herein as interrogation signals. The interrogation signals interrogate the domain which is currently being polled and any responses received from that domain are supplied (via the router 30 and interface 32) to the tag detection process. The interrogation signals which are supplied during polling of each domain allow tags within that domain to be identified. The poll database for each domain is continuously updated during polling of that domain. A time process 44 receives data from the poll database for the domain being polled and ascertains the following:

- 1) has the same tag been detected x times in y seconds? (if yes, assume tag entered domain);
- 2) same tag not detected x times in y seconds? (if yes, assume tag left domain).

The results of the time process 44 are used to update a plurality of valid detect databases 46, one database for each domain. The valid detect databases hold for each tag, the tag ID, its location, the time and date. Against each entry, a flag is set to indicate whether or not there has been a movement of that tag since the last time the database was

- 10 -

updated. Information concerning movements of tags is supplied to the data concentrater 14 via a data concentrater communication process 48. When a request is made by the data concentrater for information, the data concentrater communication process accesses the valid detect databases 46 and supplies the information concerning any flagged movements to the data concentrater.

When tags are issued at the tag issue unit 4, information is supplied to the data concentrater via the network 2 concerning the tag ID and the expiry time of that tag. That is, when the tags are used to monitor the movements of persons who have paid to enter an activity centre or the like, it is desirable to allow these persons access only for a predetermined period of time. The time after which they no longer are permitted to remain in the activity centre is entered as the expiry time. The tag IDs and expiry times are held in an expiry database 50 within the domain controller. When the expiry time of a particular tag has been reached, the identity of that tag is supplied to the tag detection process 42 which issues an appropriate signal to the router to control subsequent transmitted signals for that tag.

The domains can be polled using one of the following techniques.

The transmitted signal  $T_x$  from the domain controller includes a message which triggers all of the tags within the domain volume. Any tags within the volume then issue a response which identifies each tag uniquely. When a plurality of tags are present within the domain volume, they issue responses in a way which prevents them from interfering with one another, i.e. on different time slots or on different frequencies. This requires the use of complex detection electronics within the domain controller.

- 11 -

As an alternative, the signal  $T_x$  transmitted by the domain controller can consist of a series of codes, each code uniquely identifying a tag. Each tag has stored within it a unique code which is compared at the tag with the code transmitted by the domain controller. When the transmitted code matches the code stored within a tag, only that tag will respond.

The gates can be polled in a similar fashion. While a tag remains within zone A (i.e. the wearer does not pass through the exit/entrance zone 3 into zone B), no change is made to the data stored at the data concentrator concerning the location of that tag. The data concentrator will already hold information for that tag concerning the domain inside the physical boundary within which the tag is located. If however a tag is detected in zone B, the gate controller will immediately notify the data concentrator via the network 2 to indicate that a wearer is now outside the physical boundary.

The data concentrator 14 thus holds up-to-date information concerning the identity of each tag which has been issued at the tag issue unit with the location of that tag. This information can be accessed by a file server 8 attached to the network 2 and displayed. This means that in the event of an emergency, the location of each person within the monitored volume is known. This assists fire officers and safety personnel in their rescue attempts. Moreover, if there is an emergency evacuation, it is possible to detect, using the gate controllers, that the holders of all issued tags have left the building.

Figure 6 is a block diagram illustrating the main components of a tag. Each tag can take the form of a watch type device to be worn on the wrist of a wearer and has its own battery. Batteryless tags may also be possible, activated via received

- 12 -

signals. The tag comprises an RF receiver 70 for receiving transmitted signals  $T_x$  from the domain controller or gate controller. A diode detector 72 is connected to the RF receiver 70. Transistor circuitry 74 in the form of an emitter follower and common collector prepare the received RF signal for supply to a tag chip 76. The tag chip 76 includes an A/D converter 78 which receives the analogue signal from the transistor circuitry 74 and supplies a corresponding digital signal to logic circuitry 80. In the case where the second of the polling techniques is used, the logic circuitry compares an incoming code with a code stored on the tag and causes a response to be issued if there is a match between the incoming code and the stored code. The stored code can also be in bar coded or human readable form on the outside of the tag. The logic circuitry 80 includes a memory for storing the code and a comparator for comparing the incoming code with the stored code. The logic circuitry 80 controls a transmit antenna 82 to transmit a suitable response signal  $R_x$  when the incoming code matches the stored code. The tag additionally comprises a light emitting diode 84 connected to the output of the logic circuitry 80 via a resistor 86. The purpose of this light emitting diode is to provide a visual indication at each tag. The light emitting diode 84 can be activated from the domain controller by including an appropriate message in the signal  $T_x$  transmitted from the domain controller. In one application, a signal is transmitted to a tag identified by its unique code when the valid time on the tag has expired, as stored in the expiry database 50 of the domain controller. Thus, the light emitting diode will light up when the valid time for that tag has expired, thereby indicating to a supervisor that that person should be removed from the monitored area.

It is also possible to use the light emitting diode in emergency situations by causing a signal to be transmitted to

- 13 -

all tags including a message to activate the light emitting diode on each tag to render the wearers of the tags more visible to fire personnel or the like.

The tag monitoring system described herein has applications in many different areas where it is required to monitor the locations of persons within a site or building, e.g. workers in hazardous environments, babies in hospitals, security and access control systems.

- 14 -

CLAIMS:

## 1. A tag monitoring system comprising:

a tag issue unit for issuing a plurality of tags, each tag being uniquely identifiable;

a system controller for holding the identity of each issued tag with data identifying the location of that tag within a monitored volume;

a plurality of beacon sets defining a domain within the monitored volume, the beacons within each set each having a transmit antenna and a receive antenna for transmitting and receiving respectively electromagnetic signals in the domain, wherein beacons within one set are arranged at different locations from beacons in the other sets to substantially avoid dead zones within the domain, and wherein the system controller comprises switching means for sequentially selecting said beacon sets to poll the domain to uniquely identify any tags within the domain and to update said location data accordingly.

2. A tag monitoring system according to claim 1 wherein there are a plurality of domains, each domain being defined by such a plurality of beacon sets and wherein the system controller is operable to poll all of the domains to determine the location of tags.

3. A tag monitoring system according to claim 1 or 2 wherein the monitored volume is defined by a physical boundary having at least one exit zone, there being arranged at said exit zone an internal beacon set and an external beacon set on opposed sides of the exit zone in relation to the physical boundary to define a gate region, the system controller being operable to poll said gate region to detect when any tags leave the monitored volume.

- 15 -

4. A tag monitoring system according to any preceding claim wherein the system controller comprises a domain controller for polling the or each domain and a data concentrater for holding up-to-date information concerning the identity of each tag and its location within the monitored volume.

5. A tag monitoring system according to claim 4 wherein the data concentrater and the domain controller are separately connected to a network which allows communication between them.

6. A tag monitoring system according to claim 5 wherein the tag issue unit is also connected to said network.

7. A tag monitoring system according to claim 5 or 6 wherein there is a plurality of domain controllers, each domain controller monitoring a plurality of domains.

8. A tag monitoring system according to any preceding claim wherein each tag issued by the tag issue unit has stored therein a unique code identifying the tag, and wherein the system controller is operable to poll the or each domain by issuing a sequence of codes for transmission via the transmit antenna of the beacon sets and for awaiting any responses via the receive antennas of the beacon sets, a response being issued by a tag whose stored code matches a transmitted code.

9. A tag monitoring system according to any preceding claim wherein the system controller holds with the identification of each tag an expiry time for that tag, the expiry time representing the time at which a holder of the tag can no longer validly remain in the monitored volume and is operable to generate an expiry signal to that tag when the expiry time is reached.



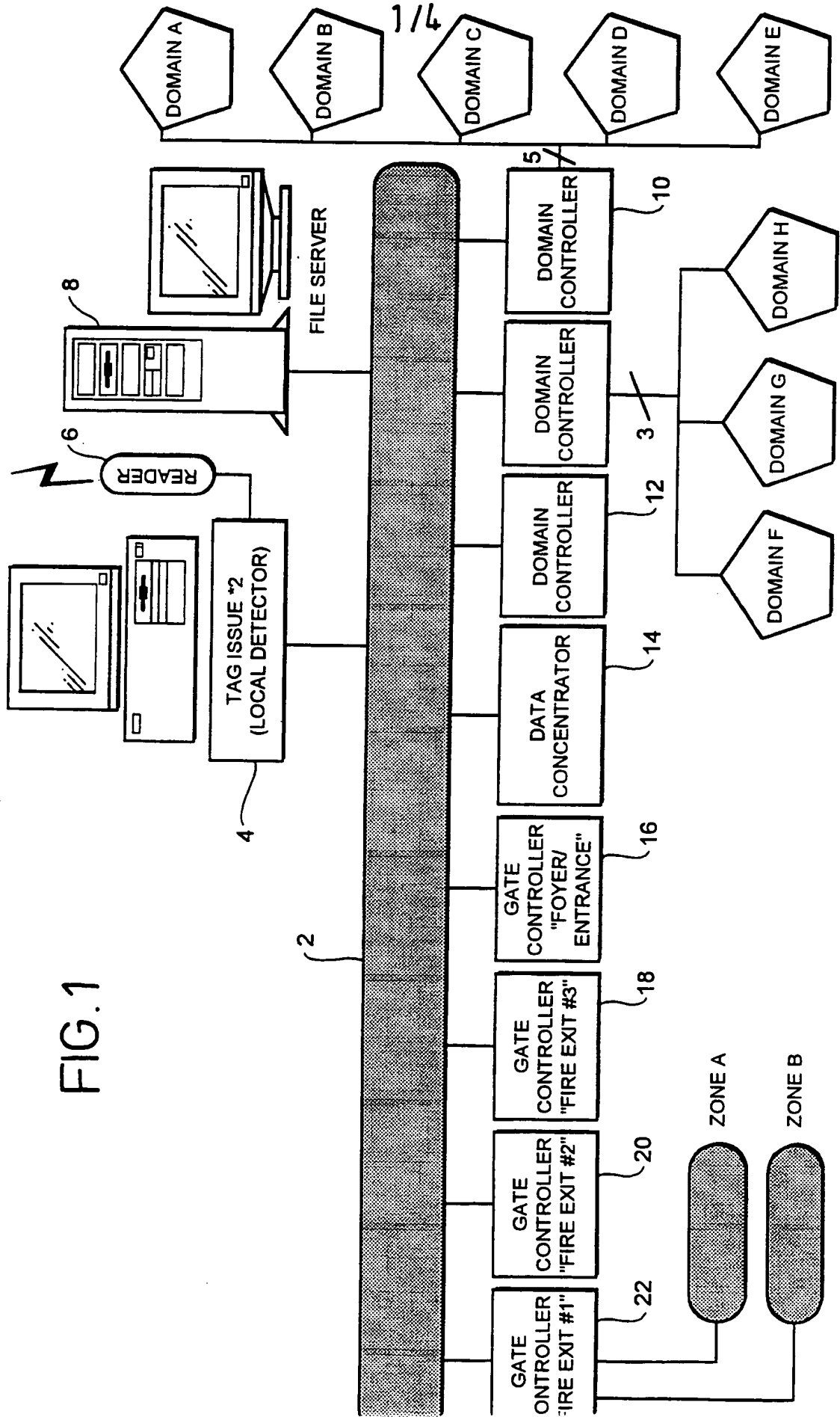
- 16 -

10. A tag monitoring system according to claim 9 wherein the expiry signal activates a visual indicator on the identified tag.
11. A tag for use in a tag monitoring system comprising:
  - a receiver for receiving an electromagnetic signal from a system controller;
  - a transmitter for transmitting electromagnetic signals as response to received signals;
  - logic circuitry for controlling the responses of the tag;
  - and
  - a visual indicator controlled by the logic circuitry so that it can be activated in response to electromagnetic signals transmitted from the system controller.
12. The tag according to claim 11 which includes a store holding a code uniquely identifying the tag and a comparator for comparing incoming codes from the system controller with said stored code, wherein a response is issued if the incoming code matches the stored code.
13. A tag monitoring system for monitoring the locations of tags within a volume, the tags being in accordance with claim 11 or 12, wherein the system controller holds the identification of each tag within the monitored volume together with expiry data denoting an expiry time beyond which the holder of the tag should no longer validly remain in the monitored volume, the system controller being operable to issue an expiry signal to a tag when its expiry time is reached, said expiry signal causing the visual indicator to be activated.

- 17 -

14. A tag monitoring system according to claim 13 when used with tags according to claim 12, wherein the expiry signal is issued with the code uniquely identifying the tag for which the expiry time has been reached.

15. A tag monitoring system according to claim 13 or 14 wherein the system controller is operable to transmit a signal to actuate the visual indicators on all tags in an emergency situation.



2 / 4

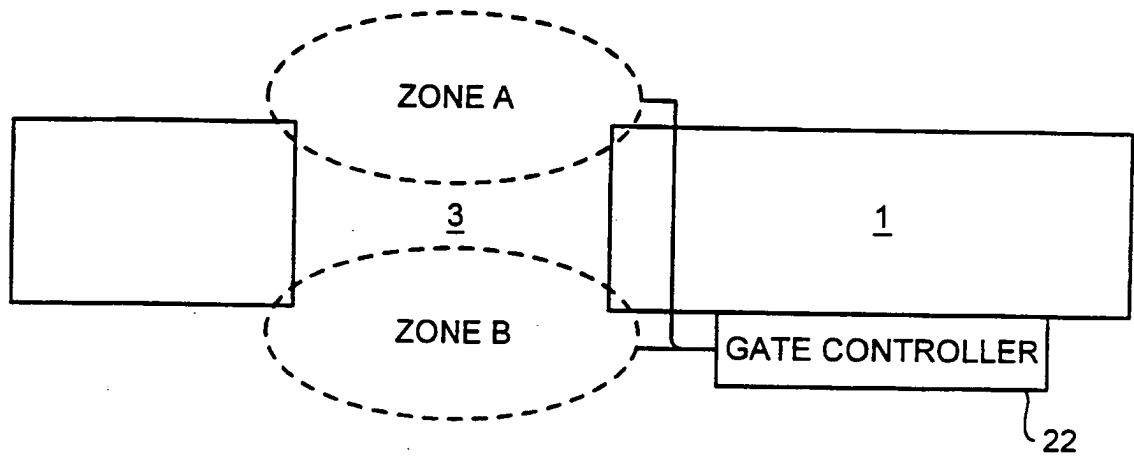


FIG. 1a

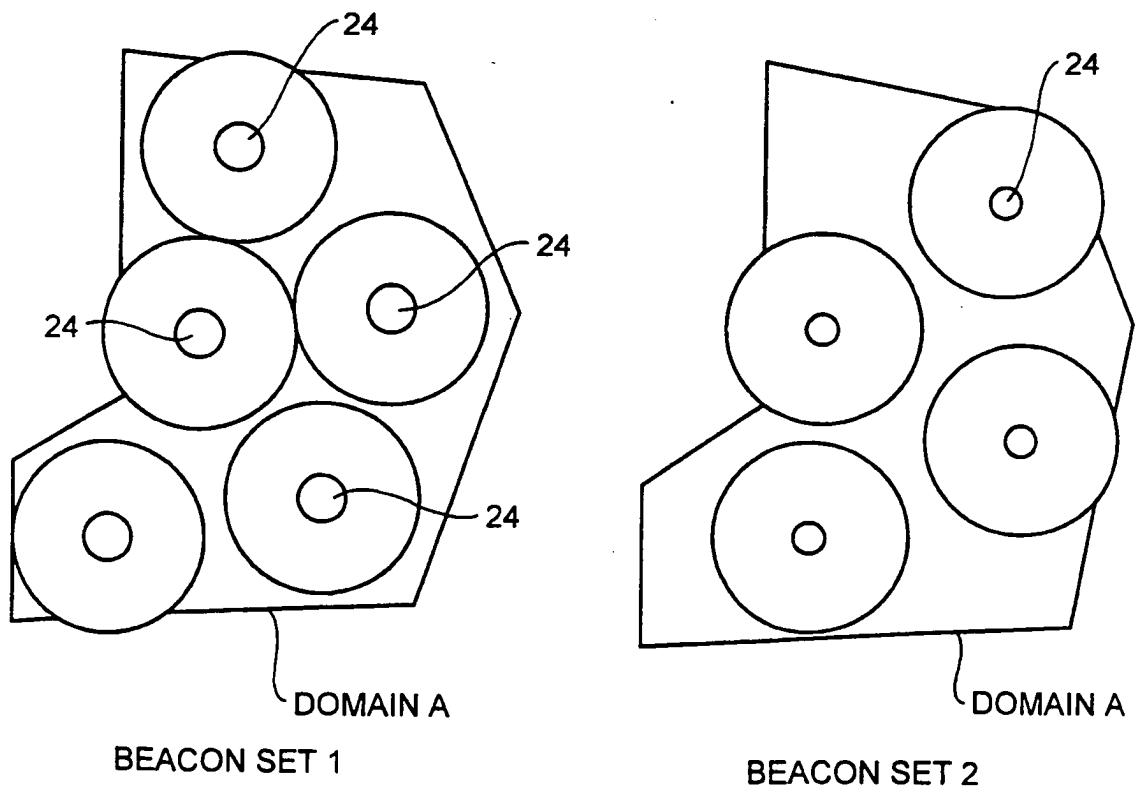
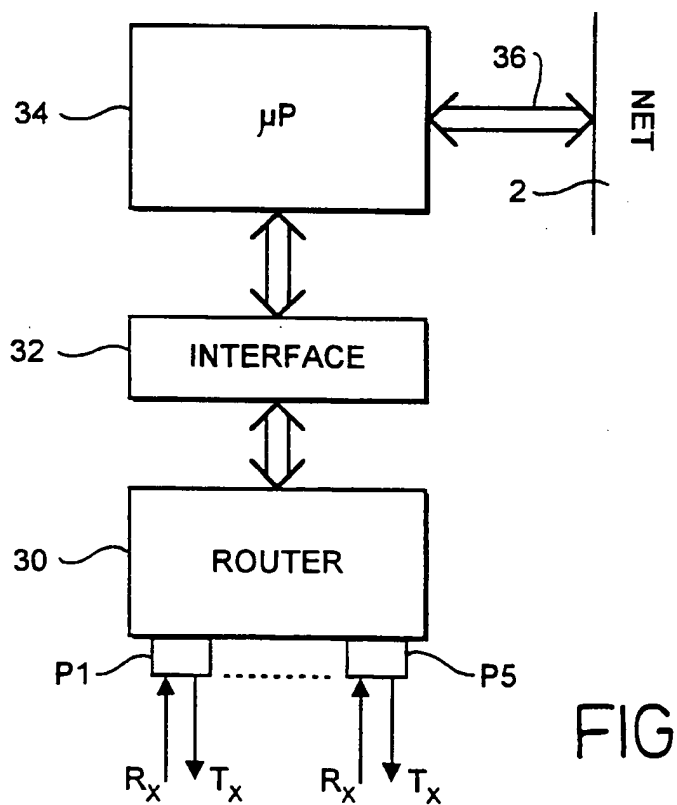
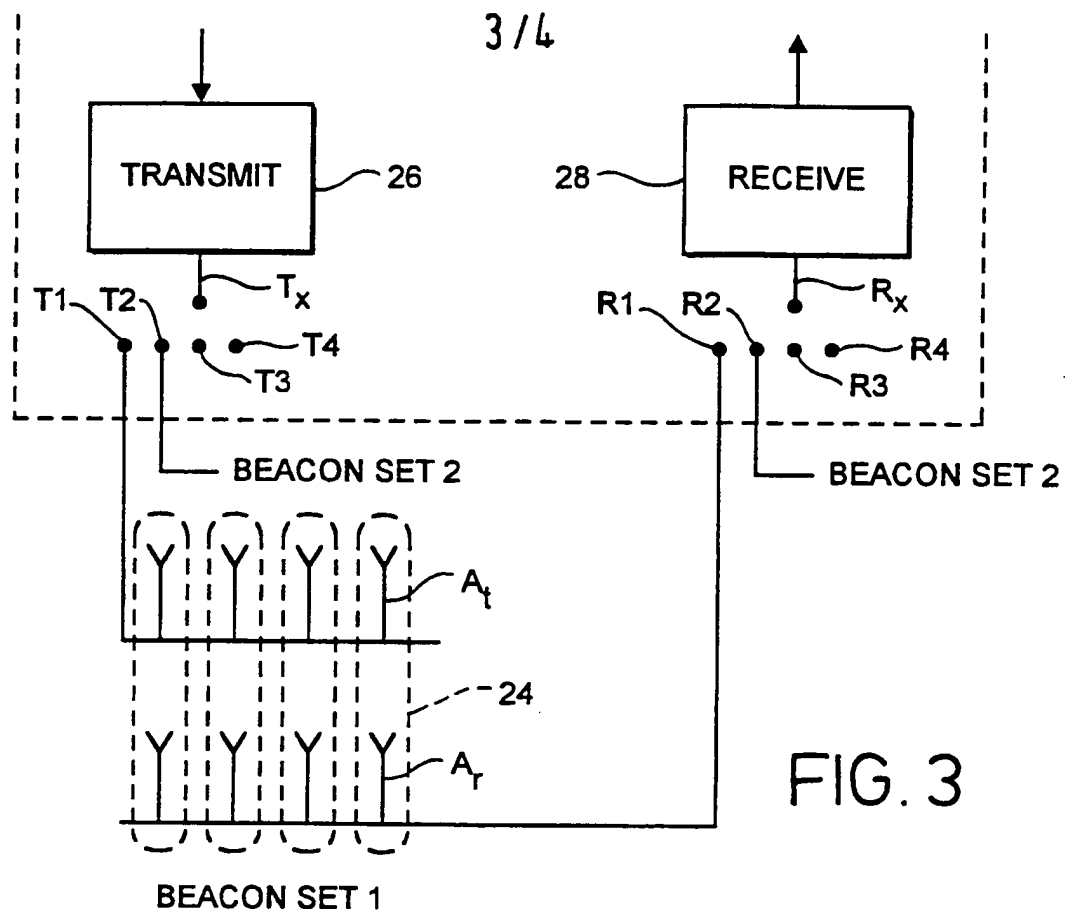


FIG. 2



4/4

FIG. 5

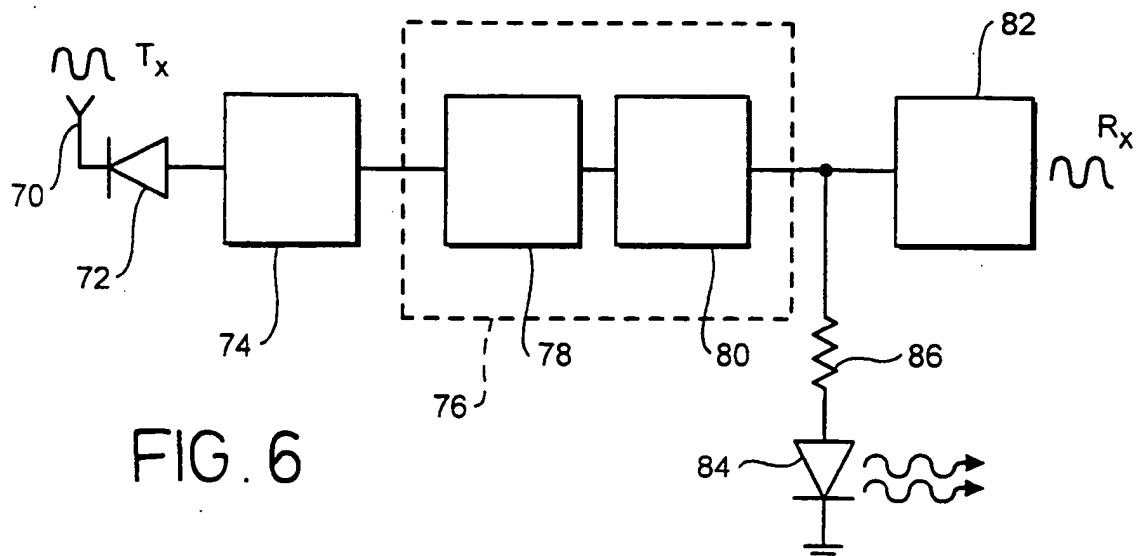
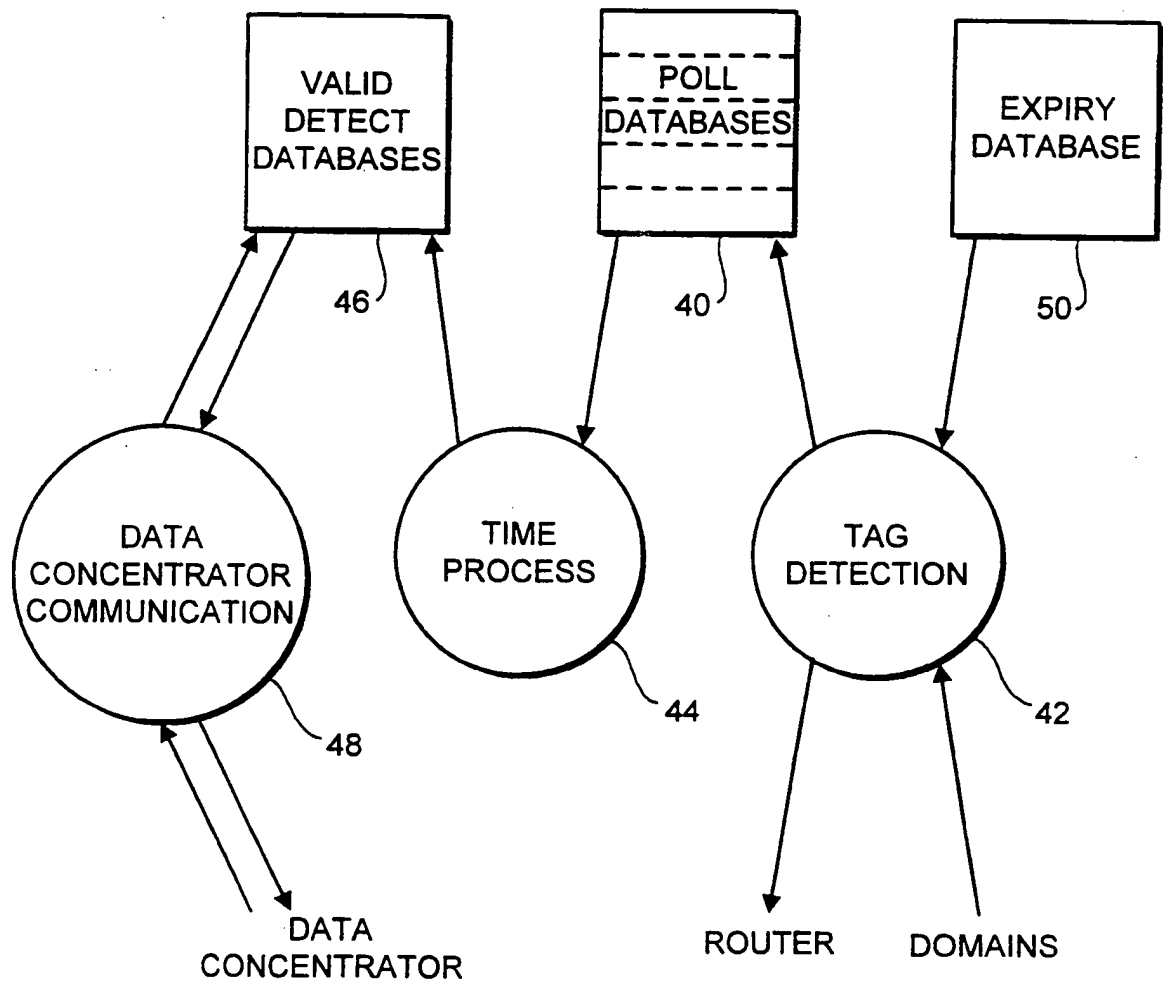


FIG. 6

# INTERNATIONAL SEARCH REPORT

Inter. Application No  
PCT/GB 96/01516

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 6 G07C9/00 G01V15/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
IPC 6 G07C G01V

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,5 218 344 (RICKETTS JAMES G) 8 June 1993 see column 8, line 34 - line 40 see column 9, line 28 - line 35; claim 1; figures 1,2	1,2,4,5, 8
A	US,A,3 478 344 (SCHWITZGEBEL RALPH K ET AL) 11 November 1969 see abstract see column 2, line 71 - column 3, line 5 see column 5, line 49 - column 6, line 20; figure 1	1,4,8
A	US,A,4 598 275 (ROSS CLIVE ET AL) 1 July 1986 see column 3, line 55 - line 62 see column 5, line 7 - line 46; figure 1	1,3
	--- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

### \* Special categories of cited documents:

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*Z\* document member of the same patent family

Date of the actual completion of the international search

2 October 1996

Date of mailing of the international search report

16. 10. 96

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentaan 2  
NL - 2280 HV Rijswijk  
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+ 31-70) 340-3016

Authorized officer

Anderson, A

# INTERNATIONAL SEARCH REPORT

Inter nal Application No  
PCT/GB 96/01516

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PATENT ABSTRACTS OF JAPAN vol. 95, no. 001 & JP,A,07 020237 (MASUO IKEUCHI), 24 January 1995, see abstract ---	1
A	US,A,4 225 953 (W.F.SIMON) 30 September 1980 see column 3, line 50 - column 4, line 29; figure 1 ---	1,6
A	GB,A,2 193 359 (MULTITONE ELECTRONICS PLC) 3 February 1988 see page 2, column 1, line 34 - column 2, line 79; figures 1,2 ---	3
A	US,A,3 923 134 (REZAZADEH REZA) 2 December 1975 see column 6, line 46 - column 7, line 8; figure 2 ---	9
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 33, no. 7, December 1990, NEW YORK, US, pages 43-45, XP002014999 ANONYMOUS: "Timed Validation Device." -----	13



# INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/GB 96/01516

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-5218344	08-06-93	NONE	
US-A-3478344	11-11-69	NONE	
US-A-4598275	01-07-86	CA-A- 1247706 EP-A- 0125143	27-12-88 14-11-84
US-A-4225953	30-09-80	NONE	
GB-A-2193359	03-02-88	NONE	
US-A-3923134	02-12-75	CA-A- 1017916 GB-A- 1468628	27-09-77 30-03-77